From: Chen, Lily (Fed)
To: Moody, Dustin (Fed)
Subject: RE: Slides update
Date: Tuesday, January 31, 2017 4:06:00 PM
Attachments: PQC-NAF-01312017A.pptx

Dustin:

Thanks. See attached.

Slide 2 - For Grover's algorithm on AES, we should probably should say "approximately" or "roughly", since it's not exactly the square root. It might be easier to say we need to double the key length. [I changed and also added something about double the key size. The point is that 2^64 quantum operations may not be as practical as classical operations.]

Slide 6 - is y missing in the 1st sentence of the 4th bullet? [Not sure about which y] or should it say something like "experience tells us that we need at least several years..." or "at least ten years..."? [see what I changed to]

Slide 6 - I assume you will explain backward secrecy [I will and I also add something in (maintain secrecy for the information encrypted x years ago), check]

Slide 8 - the last bullet you added. You can remove the bullet if you want, and just verbally tell them this is our rough timeline, which can change. [removed]

By the way, are we both giving the talk? Or just you? Or just me? I wasn't sure. Thanks, [I will give the talk. Both of us will answer questions. I am usually slower so 20 pages probably is the maximum amount for me to handle. I think we will not leave right after our talk to give people some time to ask questions offline. As the next session starts, if it is not very interesting, we can leave. What do you think?]

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, January 31, 2017 3:44 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Slides update

Lily,
Slide 2 - For grover's algorithm on AES, we should probably should say "approximately" or "roughly", since it's not exactly the square root. It might be easier to say we need to double the key length.
Slide 6 - is y missing in the 1st sentence of the 4th bullet? or should it say something like "experience tells us that we need at least several years..." or "at least ten years..."?
Slide 6 - I assume you will explain backward secrecy

Slide 8 - the last bullet you added. You can remove the bullet if you want, and just verbally tell them this is our rough timeline, which can change.
I like slides 15 and 16 and 18 and 19 as you changed them.

By the way, are we both giving the talk? Or just you? Or just me? I wasn't sure. Thanks,

Dustin

From: Chen, Lily (Fed)
Sent: Tuesday, January 31, 2017 3:22:41 PM
To: Moody, Dustin (Fed)
Subject: Slides update

Hi, Dustin:

I extended the slides a little bit. See attached.

Here is a list of changes.

1. Page 2, add the last bulletin (impact on symmetric key algorithms)
2. Page 6 is new to address the urgency
3. Page 8 add the last bulletin on the right column (possible change)
4. Page 15 and 16 are new (from my AWACS slides)
5. Page 18 change the initial actions to Hybrid mode
6. Page 19 new, other standards, include hash based signatures here

Now we have about 20 pages. I think this probably is the maximum amount we can handle in one hour since I would expect a lot of questions.

Any comments?

Lily